Janice K. Brewer
Governor

Brian C. McNeil
Director

ARIZONA DEPARTMENT OF ADMINISTRATION

OFFICE OF THE DIRECTOR

100 NORTH FIFTEENTH AVENUE • SUITE 401
PHOENIX, ARIZONA 85007

(602) 542-1500

August 15, 2014

Mr. Brian C. McNeil, Director
Arizona Department of Administration
100 N. 15th Ave.
Phoenix, AZ 85007

Dear Brian:

In response to the ***Amended*** Project Investment Justification (PIJ) for the **"Data Center Security Management"** project, my staff has reviewed your proposal to acquire additional tools and services to further cybersecurity protections for the State through expanded intrusion protection capabilities.

The original PIJ implied funding was available from the Fiscal Year 2014 (FY14) Automation Projects Fund (APF) in the amount of $710.9 thousand for the total three-year life cycle cost of the project. The amended PIJ implies additional funding is available from the FY15 APF for a total four-year life cycle cost for the project of $1,480.5 thousand.

This is notification of Arizona Strategic Enterprise Technology Office's recommendation to the Information Technology Authorization Committee (ITAC) for **Approval with Conditions** of the ***Amended*** technology project as follows:

1. Should there be a change in the proposed costs of 10% or more, the Security, Privacy and Risk (SPR) team within ADOA-ASET must amend the PIJ to reflect the changes and present it to ITAC for review and approval prior to further expenditure of funds.

The ITAC is scheduled to meet on August 27, 2014 to review this project. Should the ITAC approve the project, you may then proceed to secure additional approvals as required from the Joint Legislative Budget Committee, the Office of Strategic Planning and Budgeting, and the State Procurement Office.

Best Wishes,

Aaron V. Sandeen
State CIO and Deputy Director
Arizona Strategic Enterprise Technology (ASET) Office

jc

cc: Mike Lettman, ADOA-ASET
Nancy Brister, ADOA-ASET
Andrew Smith, JLBC
John Arnold, OSPB
Barbara Corella, SPO
Phil Manfredi, ADOA-ASET
Jeffrey Crane, ADOA-ASET

ASET# AD14004_A

Analyst: Jeffrey Crane **PIJ Summary - ASET** Project Number: AD14004_A

Agency Name & Address	*Contact Name & Phone*
Arizona Department of Administration 100 N. 15th Ave. Phoenix, AZ 85007	Mike Lettman 602-542-0030 Mike.Lettman@azdoa.gov
Project and Investment Justification Name	*Date Submitted*
Data Center Security Management	October 4, 2013 (original date) ***August 6, 2014*** (amended date)

Project Overview

Problem Description

In Fiscal Year 2014 (FY14), a number of transformation initiatives were prioritized by Governor Janice K. Brewer, proposed in her budget, and subsequently codified into law. Included in these are a series of measures designed to further protect the State against the ever-increasing threats to its systems and confidential data. While a number of security protection and risk mitigation measures were successfully implemented in FY13 by the Arizona Strategic Enterprise Technology (ASET) Office within the Arizona Department of Administration (ADOA), the State must continue to build upon these efforts. The AD13008 Cyber Security Operations Strengthening project successfully deployed technologies in the State Data Center (SDC) to automate threat management and implement intrusion detection system (IDS) functionality. However, more needs to be done to protect State data from cybersecurity threats that may be directed toward other State agency data centers that lack intrusion detection capabilities. In order to integrate and analyze information generated from multiple sources regarding cybersecurity threats, additional functionality is needed to provide consolidated, centralized reporting for ADOA and other State agencies.

Solution

In alignment with the Agency's strategic goals, ADOA is proposing to address potential threats through expanded monitoring of State internet connections, more sophisticated analytics technology, and additional automated compliance capabilities. Based on prior demonstrations, ADOA-ASET will acquire a new software solution that is able to correlate data from a variety of other individual tools to create a dashboard of the State's cybersecurity threat situation. In addition, the software will use the same input to identify regulatory compliance issues and security gaps. ADOA-ASET will also expand services currently provided by the U.S. Department of Homeland Security's Multi-State Information Sharing and Analysis Center (MS-ISAC), in order to monitor internet communications and receive alerts regarding potential threats across additional internet access points.

In FY14, ADOA acquired compliance and analysis tools that correlate data and provide a consolidated dashboard view into potential compliance issues and security threats. Additionally, monitoring services were extended to internet access points and a Security Operations Center (SOC) was established to enhance intrusion detection capabilities. ADOA is now proposing to utilize remaining FY14 and new FY15 Automation Projects Fund (APF) monies to implement additional leading edge technologies that will further cybersecurity protections through expanded intrusion detection capabilities within the Agency and across the State.

Measurements and Deliverables

ADOA-ASET will acquire a new compliance and analysis product from a vendor partner on State contract, which is designed to accept input from a variety of data streams, apply analytics technology to correlate that data, and provide a consolidated dashboard view into potential compliance issues and security threats. Before committing to its use, the Security, Privacy and

Risk team within ADOA-ASET (ASET/SPR) will conduct an initial proof-of-concept (POC) of the proposed software, to confirm viability prior to full-scale implementation. ASET/SPR will also evaluate ancillary tools needed to direct specific data feeds and devices to be monitored into the proposed software, and will select a set of applicable tools based on value and cost. Initial Licensing & Maintenance costs in the PIJ reflect a three (3) year license for the compliance and analysis software, after which ADOA-ASET will decide to continue using the product or seek a newer technology that may be available. In addition to software acquisition costs for the ancillary toolset, the PIJ includes hardware costs to acquire a dedicated server to house the software and data to be gathered. Professional & Outside Services in the PIJ include two (2) Security Operations Center (SOC) subject matter experts to assist in evaluating and operationalizing the expanded monitoring and reporting.

In addition, ADOA-ASET will extend the monitoring currently provided to the State by MS-ISAC for one (1) internet connection, to include two (2) additional internet access points. Costs to implement this service include two (2) security devices to monitor traffic across expanded internet access points, with up-front licensing for MS-ISAC monitoring services also for three (3) years. After that point, ADOA-ASET will establish either a billable service for sustainability or drop the expanded MS-ISAC service.

With the expansion of the original project scope, ADOA will research, acquire, and implement the following:

- ***Security Event Information Management System (SEIM), designed to correlate and analyze security event data in real time for internal and external threat management***
- ***Network Access Control (NAC) solution, to define and implement a policy to secure access to the State network***
- ***Server hardening tools***

The project will require an end date extension, to allow time to acquire and implement the solutions.

Benefits

The proposed compliance and analysis software will integrate information from new and existing technologies, to provide a consolidated view into potential SDC and other State data center cybersecurity threats. In addition to enhancing compliance within the SDC environment, the proposed software solution is expected to enhance incident detection and response. The ability to accept input from other State agency data feeds will allow ASET/SPR to alert those agencies regarding potential cybersecurity threats that may be detected. While MS-ISAC services already provide a high value to the State, expanding those services will allow traffic to be monitored across additional internet access points, thereby further extending protections.

These additional tools and services will enhance and expand security through a variety of intrusion detection technologies and solutions resulting in a more secure server operating environment for the State.

Project Management

The ADOA-ASET Project Manager will work with contracted and staff subject matter experts from the ADOA/SPR team to complete the project deliverables.

Enterprise Architecture

Compliant.

Original Summary of Proposed Costs

All Figures in Thousands ($000)						
Cost Description	2014	2015	2016	2017	2018	Total
Development Costs	710.9	0.0	0.0	0.0	0.0	710.9
Operational Costs	0.0	0.0	0.0	0.0	0.0	0.0
Total Project Costs	710.9	0.0	0.0	0.0	0.0	710.9

Amended Summary of Proposed Costs

All Figures in Thousands ($000)						
Cost Description	2014	2015	2016	2017	2018	Total
Development Costs	710.9	769.6	0.0	0.0	0.0	1,480.5
Operational Costs	0.0	0.0	0.0	0.0	0.0	0.0
Total Project Costs	710.9	769.6	0.0	0.0	0.0	1,480.5

Recommendation: **Approval with Conditions**

1. Should there be a change in the proposed costs of 10% or more, the Security, Privacy and Risk (SPR) team within ADOA-ASET must amend the PIJ to reflect the changes and present it to ITAC for review and approval prior to further expenditure of funds.